

LA-UR-22-21404

Approved for public release; distribution is unlimited.

Title: NSRC New Hire Orientation Resources and What to Expect

Author(s): Templeton, Patricia A.

Intended for: Training guide for new hires within the National Security Research Center

Issued: 2022-02-17



Los Alamos National Laboratory, an affirmative action/equal opportunity employer, is operated by Triad National Security, LLC for the National Nuclear Security Administration of U.S. Department of Energy under contract 89233218CNA000001. By approving this article, the publisher recognizes that the U.S. Government retains nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or to allow others to do so, for U.S. Government purposes. Los Alamos National Laboratory requests that the publisher identify this article as work performed under the auspices of the U.S. Department of Energy. Los Alamos National Laboratory strongly supports academic freedom and a researcher's right to publish; as an institution, however, the Laboratory does not endorse the viewpoint of a publication or guarantee its technical correctness.

NSRC New Hire Orientation

Resources and What to Expect

Prepared by:

The National Security Research Center at Los Alamos National Laboratory LANL is managed by Triad National Security, LLC for the U. S. Department of Energy's NNSA.



Los Alamos National Laboratory, an affirmative action/equal opportunity employer, is managed by Triad National Security, LLC, for the National Nuclear Security Administration of the U.S. Department of Energy, under contract 89233218CNA000001. By acceptance of this article, the publisher recognizes that the U.S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or to allow others to do so, for U.S. Government purposes. Los Alamos National Laboratory requests that the publisher identify this article as work performed under the auspices of the U.S. Department of Energy. Los Alamos National Laboratory strongly supports academic freedom and a researcher's right to publish; as an institution, however, the Laboratory does not endorse the viewpoint of a publication or guarantee its technical correctness.

Contents

DIRECTOR’S LETTER	1
WELCOME	2
WHERE YOU WORK	3
Introduction	3
Organization Charts.....	3
NSRC Contacts	7
Additional Contacts	7
BEGINNING WORK	8
Before (or Possibly on) Your Start Date	8
Initial Procedures.....	8
LANL RESOURCES	10
Lab Intranet	10
Listservs	10
Additional Links.....	10
GOALS	11
Continuing Professional Education Program	11
Performance Management.....	11
PROFESSIONAL DEVELOPMENT	12
Confluence	12
Utrain.....	12
Lab History Starter Kit.....	12
Libraries and Museums	12
Archives/Preservation	13
SAFETY	14
SECURITY	15
TIPS	16
Lab-specific.....	16
Local Life	18
APPENDIX A: Additional Security Information	
APPENDIX B: DOE “NO COMMENT” Policy	

Director's Letter

Colleague,

Welcome to Los Alamos National Laboratory and the National Security Research Center!

The NSRC is the Lab's classified library which also curates unclassified legacy materials from the Lab's fascinating history. We trace our lineage to the technical library the Lab's first Director, J. Robert Oppenheimer, opened in 1943 as part of the Manhattan Project in Los Alamos. Today, the Center is one of the largest technical and scientific libraries in the country, with collections that number tens of millions and span the nation's entire nuclear weapons history.

We're staffed with expert, highly trained teams of librarians, archivists, digitizers, historians, and communications specialists. We support a broad range of researchers within the Lab's Weapons Program and beyond. The NSRC also has customers across the National Nuclear Security Administration's labs and sites, as well as partners in the Department of Defense.

You've come to the Center during a time of unprecedented growth. In just the past few years, we've stood up seven new digitization labs and are in the process of adding more. We've also made historical education and outreach a significant part of our work, publishing weekly articles that highlight Lab history; producing an annual magazine; developing video documentaries; creating podcasts; designing posters; and writing historical non-fiction books. Additionally, the NSRC is implementing artificial intelligence / machine learning technologies to help index and catalog our digital collections. All of these areas are being evaluated by the NNSA for potential implementation at the other national labs and sites, solidifying our prominent role in national security mission work.

I'm confident you will be a valuable member of the NSRC team and will make important contributions to the Lab while also fulfilling your own professional goals. I look forward to working with you.

Warm Regards,



Rizwan Ali
Director, National Security Research Center

Welcome

Hello, New Hire! Right now, you are likely very excited to begin your position at the Laboratory. We are happy you are here!

This document will walk you through different facets of your pre-security clearance interval at the Lab. This is a general guide not firm documentation. Its contents were compiled by National Security Research Center (NSRC) team members to make your transition easier.

To begin, you will need a security clearance to do your job. A security clearance is essentially an extremely detailed background check. After you complete and turn in your security paperwork, the clearance process can take as little as three months or as long as one year.

You may wonder, “If I can’t do my job until after I receive a clearance, what will I be doing?” There is plenty of unclassified work and professional development to be done. Waiting for a clearance can be trying, but we are here to help. This guide details what to expect during pre-clearance, resources to stay industrious, entry points to Lab networking and culture, and tips for success.

Patience, flexibility, and productivity are key. Your workday responsibilities and priorities will vary depending on the self-study, assigned duties, and client-driven projects designated by your manager.

This guide is here to help, and so are your NSRC colleagues.

Where You Work

Introduction

You work at the National Security Research Center, the world's most comprehensive collection of nuclear weapons and national security materials dating back to the Manhattan Project. We are housed in the National Security Sciences Building (NSSB). Our classified library contains tens of millions of documents, films, books, and other materials related to the development, testing, and production of nuclear weapons. This multidisciplinary collection includes technical information related to physics, chemistry, engineering, material science, intelligence, and national security. Our collections directly support cleared researchers in achieving Los Alamos National Laboratory's (LANL) mission of solving national security challenges. Researchers come from within LANL's Weapons Program, across other National Nuclear Security Administration (NNSA) labs and sites, and partners in the Department of Defense (DoD).

The NSRC contains archival collections but is categorized as a **classified library**. We collect, arrange, preserve, and make accessible Lab resources that serve as the foundation of LANL's future innovations in the stewardship and development of nuclear weapons. The NSRC was founded in 2019. On a project by project basis, indexing and metadata standards are being established according to in-house needs and international standards. We differ from publicly accessible (university) libraries and archives due to the sensitive nature of our collections, our digitization priorities being set by customer demand, and our main outreach functions being directed at a contained demographic with a Need to Know. Though we diverge from public memory institutions, we hold in common that our staff is made of expert archivists, librarians, and information professionals who work toward refining processes, enhancing program management, and growing partnerships and collections to vibrantly engage users.

Organization Charts

Organization charts quickly go out-of-date. These charts do, however, demonstrate how the NSRC fits within the Lab. The NSRC is a project of the Weapons Research Services Division (WRS) of the Weapons Physics Directorate.

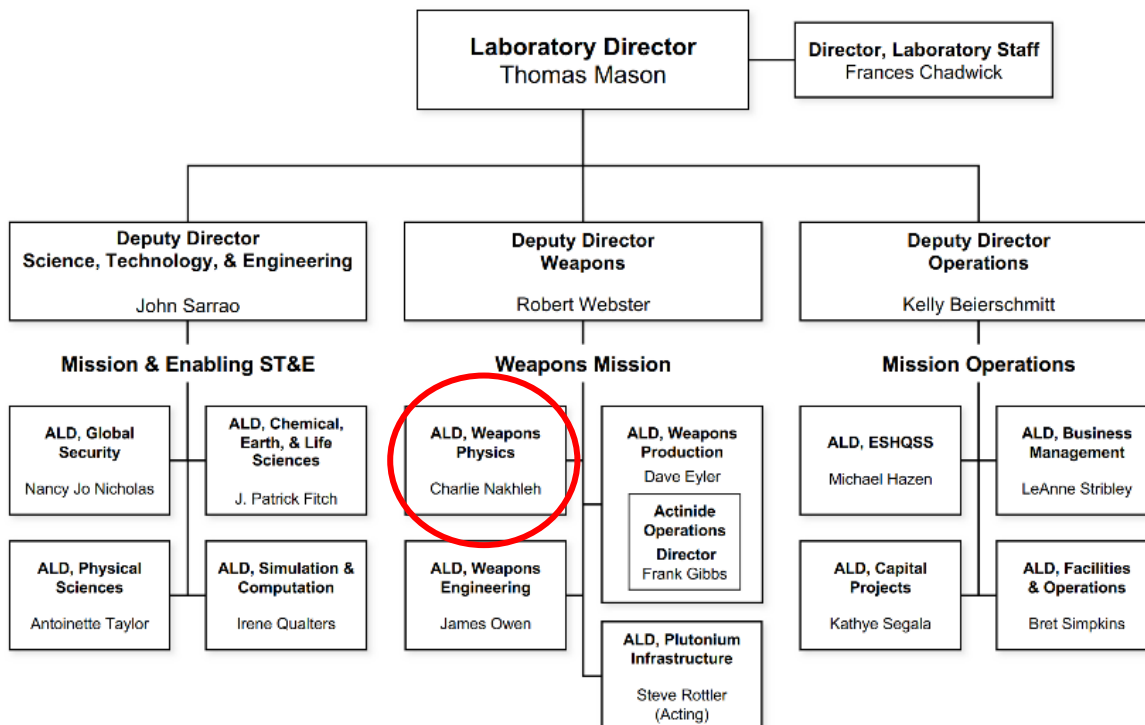
Weapons Research Services is sometimes shortened to WRS and sometimes to WRS-DO. The DO stands for Division Office.

WRS has five groups within it. The two groups that directly support the NSRC are the National Security Research Center Digital Collections group (NSRC-DC) and the National Security Research Center Mission Support group (NSRC-MS).

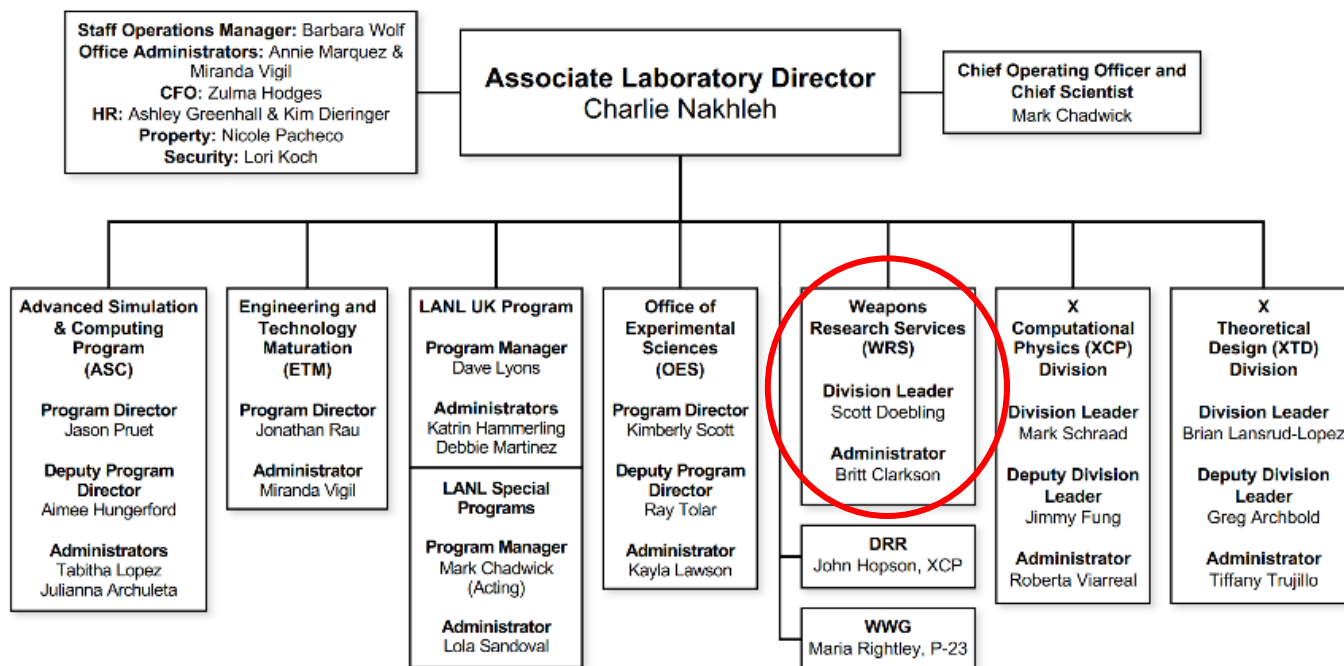
Click [here](#) for more information on Lab-wide organization charts.

Click [here](#) for more information on Weapons Research Services (ALDX WRS).

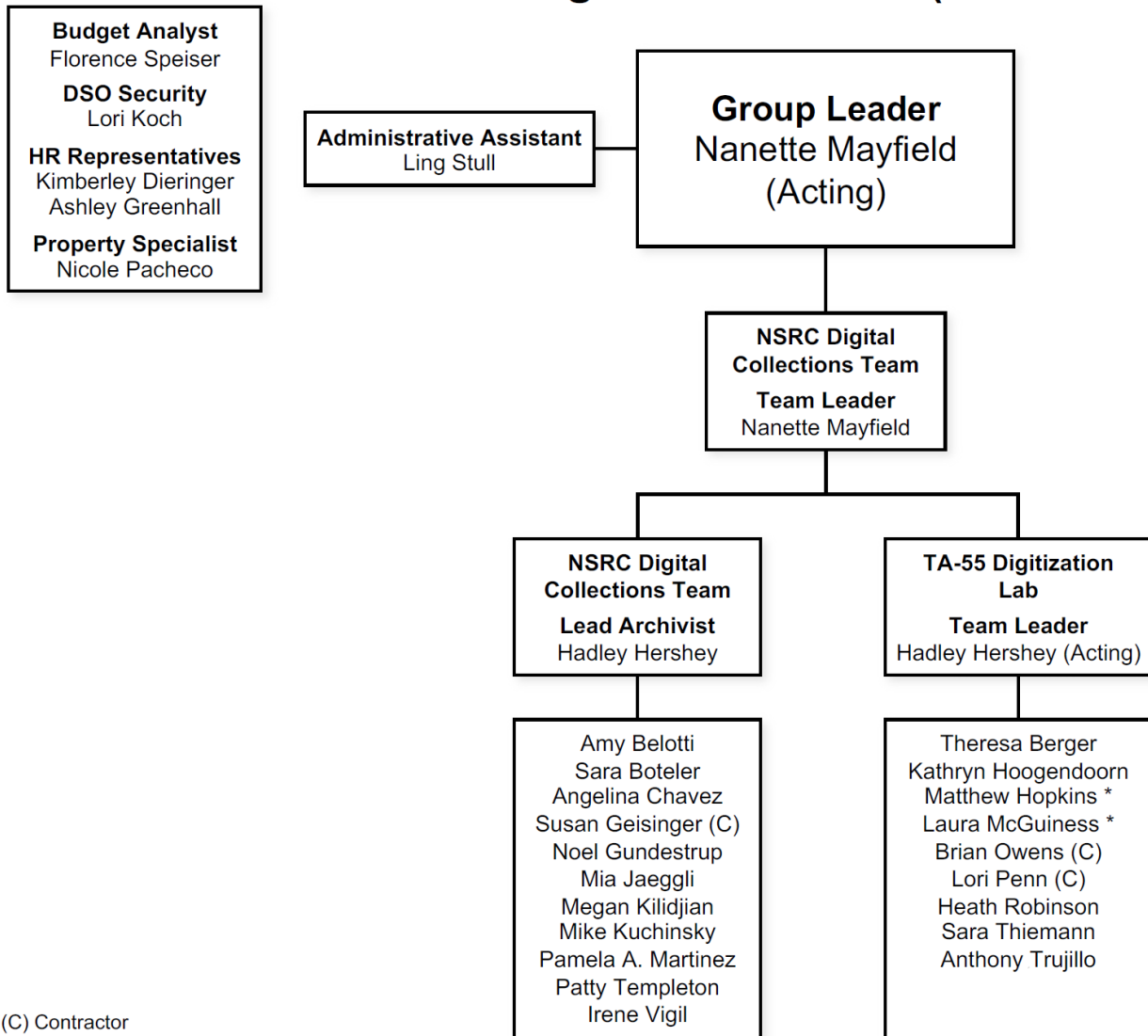
Los Alamos National Laboratory



Weapons Physics Directorate



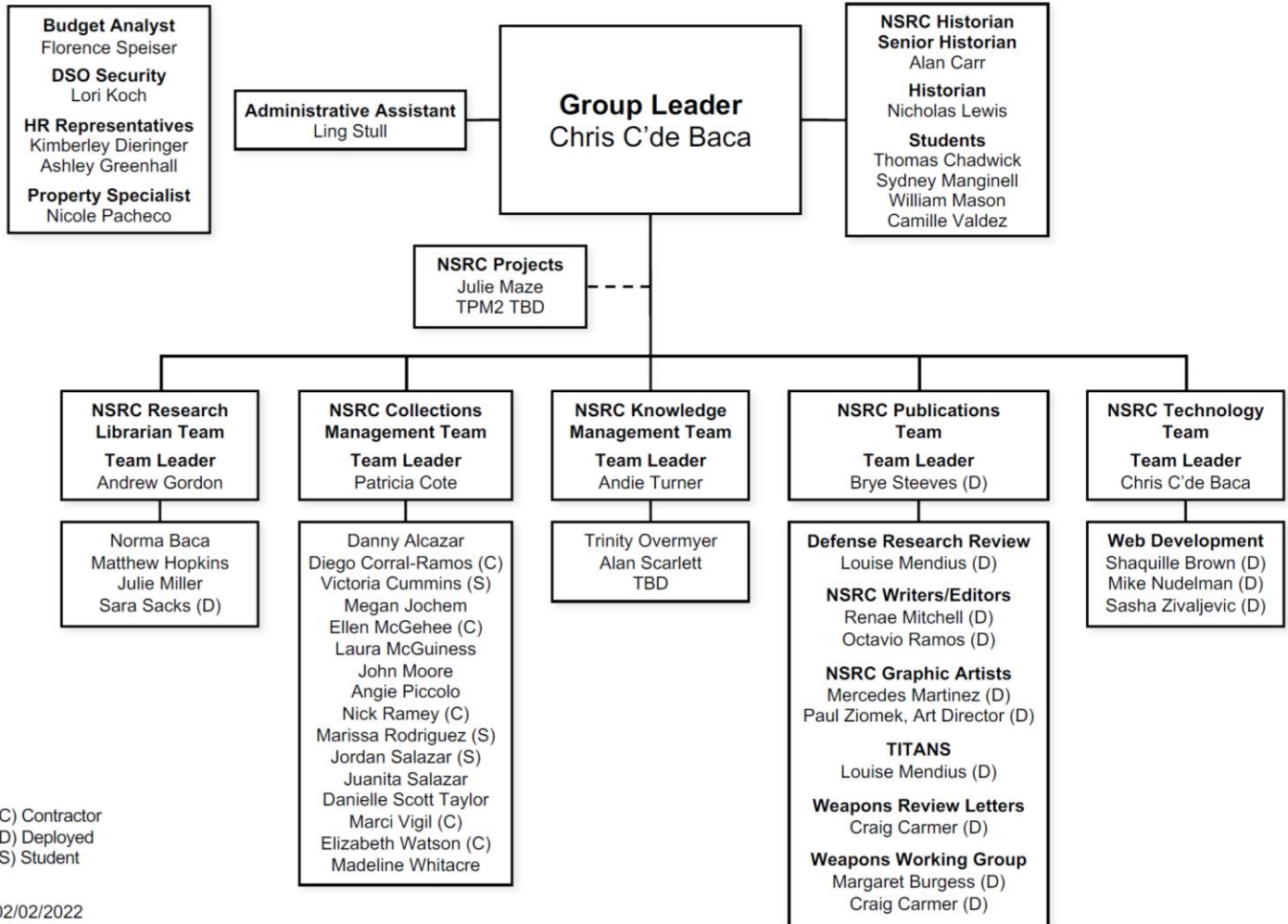
Weapons Research Services NSRC Digital Collections (WRS-NSRCDC)



(C) Contractor

* Under WRS-NSRCMS

Weapons Research Services NSRC Mission Support (WRS-NSRCMS)



NSRC Contacts

It will take time to meet members of WRS and colleagues across the Lab. WRS contains five groups. Those groups each contain teams. Each team is reliant on the other but not entirely intermixed. As you get involved with different types of pre-clearance work, you will meet others. Everyone in the NSRC has a specialty. Some of these are pointed out below, others you will be directed to on an as-needed basis.

- NSRC Director: [Rizwan Ali](#)
- WRS-NSRC-MS Group Leader: [Chris C'de Baca](#)
 - Chris approves vacation, business travel, and other funded activities along with Nanette. Chris is your **Responsible Line Manager (RLM)**. He is also a **Derivative Classifier (DC)**.
- WRS-NSRC-DC Acting Group Leader : [Nanette Mayfield](#)
 - Nanette approves vacation, business travel, and other funded activities with Chris. She is your day-to-day managerial contact if you are in the NSRC-DC group
- NSRC-DC and NSRC-MS Executive Assistant: [Ling Stull](#)
 - Go to Ling for questions about Lab processes. She is your **Point of Contact (POC)**.
- Digital Collections Team Lead Archivist: [Hadley Hershey](#)
- Collections Management Team Leader: [Patricia Cote](#)
- Research Librarian Team Leader: [Andrew Gordon](#)
- Senior Historian: [Alan B. Carr](#)
 - Alan is a fount of LANL history. Contact him about historical research projects.
- Archivist: [Danny Alcazar](#)
 - Danny is the accessioning archivist. Contact him with questions about collections, the Freedom of Information Act (FOIA), and the NSRC Vault Type Room (VTR). Danny is also a **Derivative Classifier (DC)**.
- Image Archivist: [John Moore](#)
 - To source still images, start with the History Resources drive and John. John is also a **Derivative Classifier (DC)**.
- Publications Team Leader: [Brye Steeves](#)
 - Brye handles all NSRC podcasts and publications. Contact her about writing projects.

Additional Contacts

- WRS Division Leader: [Scott Doebling](#)
- WRS Executive Admin: [Britt Clarkson](#)
- Human Resources NSRC: [Kimberley Dieringer](#)
- Security DSO/CMPC: [Lori Koch](#)
 - **DSO = Deployed Security Officer**. **CMPC = Primary Classified Matter Custodian**.
- WRS-DO Acting Chief of Staff: [Julie Maze](#)
- Property Specialist: [Nicole Pacheco](#)
- Cyber Security ISSO/OCSR: [Chrislynn Bingham](#)
 - **ISSO = Information System Security Officer**. **OCSR = Organizational Computer Security Representative**.
- Cyber Security Support: adxcyber@lanl.gov
- Local Yellow IT Support: [Bart Daly](#) and [Jessica Fernandez](#)
 - You can also send an email to askit@lanl.gov or call 505-665-4444.
- Red Computer Support: wslanhelp@lanl.gov (Team Lead: [Javier R. Martinez](#))

Beginning Work

Before (or Possibly on) Your Start Date

Your group's executive assistant will contact you with instructions about procuring a:

- ☐ LANL badge
- ☐ Z Token
- ☐ Cryptocard (these are being phased out – you may not receive one)
- ☐ Laptop

Additionally, [Human Resources](#) will contact you about a Los Alamos National Laboratory (LANL) new hire orientation.

Initial Procedures

These activities will happen swiftly and may overlap. Some are in-person, but many can be done remotely. This is not an all-inclusive list. You can research these topics by using the LANLInside search function. Please direct questions to your group's executive assistant, Human Resources, or to your manager. Within the first few weeks of your start date, plan to complete the following:

- ☐ Attend Human Resources new hire orientation
- ☐ Submit Human Resources orientation paperwork
- ☐ Complete [badge](#), [Z Token](#), fingerprinting, and drug test appointments (usually on same day)
- ☐ Procure work laptop from [EasyIT](#)
 - EasyIT will assist you in creating an email, required passwords, and a VPN
 - Complete Property Transfer Request ([PTR](#)). You must complete a PTR to take Lab devices off Lab property
- ☐ Tour of the NSRC with a supervisor
- ☐ The executive assistant will contact you about **Oracle**, **Time and Labor (T&L)**, and **performance management** training
 - Oracle is the application used to view/change personal employee information
 - T&L is where you will input weekly timecards with specific cost codes the executive assistant provides
 - Performance management records employee productivity during the fiscal year (FY)
- ☐ Decide on a [work schedule](#) and gain manager approval
 - Either you or your manager will change your work schedule in Oracle
 - Your default schedule is 5/40. This is 5 workdays (Monday – Friday) equaling 40 hours.
 - Many Lab employees choose a 9/80 schedule. This is 9 workdays equaling 80 hours. You receive every other Friday off by working longer days. Your lunch is not included in your workday. You're assigned A Friday or B Friday off by your manager.
 - Example: Monday – Friday, 7:30 a.m. – 5 p.m. with A Schedule Fridays off
 - Staffing needs may affect your ability to choose a 4/10 schedule
- ☐ Enroll in [benefits](#)
- ☐ Review/update emergency contacts in Oracle
- ☐ Complete [relocation paperwork](#) for reimbursement
- ☐ Complete [General Employment Training](#) (GET) and exam (Utrain Course #43114)
- ☐ Complete all other assigned [Utrain](#) courses and Lab/Group-assigned training activities

- Utrain is LANL's official training platform.
- Attend new hire security briefing(s)
- A personal security officer will contact you with clearance processing guides and paperwork
 - Do not delay in completing paperwork, but do not "hurry through it" sacrificing accuracy
 - Dependent on your background, this paperwork may take a long time to fill out
 - Notify references they may receive a text, email, phone call, or physical visit about you
- If your manager has not given you access to [Confluence](#), request access
- Create an [email signature](#)
- Your manager will contact you about creating work achievement goals for Performance Management
- The executive assistant will contact you about getting a Lab cell phone and/or routing work calls to your personal phone
- Schedule a remote and/or onsite [ergonomic evaluation](#) (optional)
- Request Google Workspace approval from manager and procure from <https://software.lanl.gov>
- Begin **professional development** after all required training and paperwork is completed
- Request a meeting with your group leader and/or manager to discuss performing **unclassified duties** that align with your interests
 - Examples: Writing articles for the NSRC, library book-shifting projects, indexing, or historian-related projects

LANL Resources

Lab Intranet

[LANLInside](#) has extended resources to support employees. When you open a web browser on a Lab computer, this page should be the first one you see. It contains useful links. Such as:

- [Oracle/T & L](#)
- [Utrain](#)
- [Phonebook](#)
- [Maps](#)
 - If you need to find a LANL building, go to the LANL Locator on the Maps page and search for the building you need. It is helpful to know the building number. For instance, the National Security Sciences Building (NSSB) is where the NSRC is housed and the building number is TA-03-1400. If you are being directed to a building, you can always ask for the building number to get better directions.

Take your time looking through LANLInside. It features Lab-related articles, daily news, security updates, and more. The homepage search bar in the top right corner is a great starter place if you are searching for a group, training, or anything in particular.

Listserves

Email groups and listservs you may want to sign up for include:

- Sign up [here](#) for the Research Library's newsletter
- Subscribe to new hire and early career employee events by emailing connect-leaders@lanl.gov
- Subscribe to Physics/Theoretical Colloquium events by emailing ptcolloquium@lanl.gov

Additional Links

- [Discover LANL](#)
- [National Security Research Center](#)
- [New Employee Resource Page](#)
- [Computing Home](#)
- LANL onsite [taxi service](#)
- [Acronym Database](#)

Goals

There are two goal sets for you to track: **Continuing Professional Education** credits and **Performance Management**. Track progress on goals pre and post-clearance. These goal sets are separate from monthly project metrics you are requested to track and submit.

Continuing Professional Education Program

The NSRC requires staff to achieve 24 continuing professional education credits (CPEs) in a fiscal year.

- You must have credits in at least three separate categories
- Credits must be approved of by your manager
- CPEs will be turned in before the end of the fiscal year

If you are not emailed CPE information by a supervisor, information can be found on [Confluence](#). The two forms (an overview and a tracking spreadsheet) may change, so check in with your manager and/or the executive assistant if the most recent version is not posted.

While waiting for your clearance, you may have a significant amount of time to gain CPE credits. Post-clearance, space out gaining these credits instead of “crunching” them in at the end of the fiscal year.

Performance Management

Performance management is required by LANL. This mid-year and end-of-year review is, [used](#) to develop the capacity of people to meet and exceed expectations and to achieve their full potential to the benefit of themselves and the Lab. Merit increases (which begin in January) are largely based on this process.

If you do not receive a performance management form and an instruction form on inputting goals into Oracle during your first several weeks, email the executive assistant to request them.

You will track eight goals. Of these:

- Five goals are pre-set to reflect Lab [behavioral values](#)
- One is pre-set to meet a group standard (Example: customer service)
- Two are set by you as work achievement goals. Your manager and group leader must approve these goals

You will have a mid-year review with your group leader. You will both record comments about your progress in Oracle. You will also have an end-of-fiscal-year review with your group leader. You will both, again, input comments about your progress in Oracle.

When creating goals, once you click the "Apply" or "Apply and Create Another" button goals CANNOT be changed or deleted. It is recommended that employees draft goals in a Word document, then input them into Oracle after group-leader approval.

- Fiscal year Performance Management [Timeline](#)
- Performance Management [Guides](#)
- While you are uncleared, it is important to set attainable goals that don't necessarily involve being onsite.
- Performance Plan [Template](#)
- LANL suggests that you set [SMART Goals](#). (Specific, Measurable, Achievable, Relevant, and Timely). Find the SMART Goals worksheet, [here](#).

Professional Development

It is up to the employee to conduct self-directed professional development between assigned duties and client-driven projects pre and post-clearance. A wide variety of resources have been gathered to set you up for success in learning the history and science of the Lab and to further your job skills.

You may read, watch, or listen to resources not mentioned here, but they must directly relate to your job function. If you have questions if a resource is appropriate, email your manager for approval. Additionally, if you wish to attend a conference, certificate program, or other learning experience requiring funding, ask for manager approval before registering for the event.

Your professional development activities count toward your CPE credits.

Keeping an activities spreadsheet may be useful but is not required. Categories can include webinars, books, Utrain courses, etc. You will probably be required to send a weekly status report to your manager. Keeping a spreadsheet can help with this check-in and with writing your mid and year-end reports.

Confluence

The [WRS Confluence site](#) is a knowledge sharing space for NSRC personnel. Spend time familiarizing yourself with it, particularly the [Professional Development](#) section. For example, if you want to brush-up on your historical knowledge of the Lab see: the [Manhattan Project](#) section and the [History](#) section.

If you want to suggest a resource to be added to Confluence, email your manager.

Utrain

Useful [Utrain](#) courses you can assign yourself include:

- Course **#47828**, **#47829**, **#47830** and **#47831** about the performance management process, including guidance for writing goals that align with the Lab Agenda and the role of behaviors in job performance.
- Course **#12985**. You can't climb a ladder in the NSRC's (very tall) classified library until you take this. It is a live WebEx class and only offered every several months. Sign up ASAP.

Lab History Starter Kit

Here is a short list of resources that your colleagues found useful when beginning at the Lab:

- Book: *109 East Palace*, Jennet Conant
- Book: *The General and the Genius*, James Kunetka
- Book: *The Making of the Atomic Bomb*, Richard Rhodes
- Book: *American Prometheus*, Kai Bird and Martin J. Sherwin
- Book: *The History of the Los Alamos National Security Research Center Collections*, Michael P. Bernardin and Alan B. Carr (available [here](#))
- Movie: *The Bomb*, 2015 (available through YouTube)
- Movie: *Trinity and Beyond*, 1995 (available through Research Library)

Libraries and Museums

Bradbury Science Museum, Los Alamos, NM

- Collections Specialist contact: [Wendy Strohmeyer](#)
- The Bradbury accessions Lab artifacts whereas the NSRC accessions Lab documents and media

LANL Research Library

- The [Research Library](#) is in the J. R. Oppenheimer Center along with EasyIT. It is open 24/7 to badge holders and has a great collection of LANL-related materials. You can peruse the collection onsite (in the basement), via [LibGuides](#), or through the [catalog](#).

Los Alamos History Museum, Los Alamos, NM

- Archivist contact: Rebecca Collinsworth. Email: archives@losalamoshistory.org; phone: 505-695-5252
- You may see the Los Alamos History Museum referred to as the Los Alamos Historical Society
- The NSRC and the LAHS do not have a reciprocal relationship. For example, if an image is required for a LANL article, there is a fee schedule related to obtaining that image

Mesa Public Library, Los Alamos, NM & the White Rock Branch

- If you don't live in Los Alamos, you may still borrow materials from the Mesa Public Library by requesting a guest (library) card. Check out their Digital Library for ebooks and audiobooks.

National Museum of Nuclear Science & History, Albuquerque, NM

NSRC collections

- The NSRC has a collection of archival resources, media, and a Special Collection. To search for books, use the Research Library's [catalog](#). Items with the location "NSRC Book Collection" should be requested from nsrc@lanl.gov. The Special Collection includes a Professional Resources Collection with most of the books on the Academy of Certified Archivists exam reading list and other archival and preservation-specific books.

New Mexico History Museum, Santa Fe, NM

Santa Fe Public Library, 3 branches in Santa Fe, NM

- If you have a library card from any New Mexico public library, you may check out materials at the Santa Fe Public Library. Check out their Digital Library resources for ebooks and audiobooks.

[Archives/Preservation](#)

Here are helpful links your colleagues turn to. If you would like a resource about a specific media type, reach out to your team members. (You may have to **right-click to copy/paste external links** into a browser due to LANL security authorizations.)

- [Society of Southwest Archivists](#)
- Society of American Archivists
 - [Continuing education](#) resources (Example: Digital Archives Specialist certificate)
- Academy of Certified Archivists
 - ACA certification [exam](#)
- [Association of Moving Image Archivists](#)
- [Association for Library Collections and Technical Services](#)
- [Connecting to Collections Care](#)
- [Conservation Center for Art and Historic Artifacts](#)
- [Council on Library and Information Resources](#)
- [Digital Preservation Coalition](#)
- [Image Permanence Institute](#)
- [National Film Preservation Foundation Guide](#)
- [Northeast Document Conservation Center](#)

Safety

Every Lab worker has the right to pause or stop work, without reprisal, because of a reasonable belief that the task poses a safety, health, environmental, procedural, security or waste generation concern, or an imminent danger or other hazard for which there is insufficient time to seek effective redress through the normal reporting and abatement process. Click [here](#) for more information.

The top four causes of injury at the Lab are repetitive trauma, slips/trips/falls, push/pull/lift, and struck by/struck against injuries. Click [here](#) for ideas on controlling hazards associated with work injuries.

Outdoor safety hazards at LANL include [weather](#), which may change rapidly. Outside of Florida, the mountains in Northern New Mexico receive the most recorded lightning strikes in the country. Wintertime brings icy driving conditions and slippery parking lots. Summer heat can lead to sunburns and dehydration. Check the forecast and prepare for anticipated weather conditions when walking, driving, or working outdoors.

Wildlife encounters are a part of Lab life. Coyote, deer, elk, bear, and the occasional mountain lion sighting are reported every year along with endangered birds, venomous snakes, and biting insects. We even have [feral cattle](#). Click [here](#) for more information.

Sometimes rodents can become a problem in Laboratory facilities, particularly in older facilities and storage spaces. For mice or other pests in a building, contact Pest Control at 505-667-6111.

Contact the Laboratory 24/7 Emergency Operations Support Center (EOSC) at 505-667-2400 for assistance with or information about all non-life-threatening situations that involve abnormal or unusual circumstances. Click [here](#) for more information.

Any worker can submit a facility service request for maintenance needs. Click [here](#) for more information.

Security

The group/division deployed security officer (DSO) is [Lori Koch](#). The DSO provides interpretation and clarification of LANL security policies on just about every security subject, including physical, personnel and cyber security, and classified matter protection and control. After hours, you should page the Lab security duty officer at 505-949-0156 for assistance and reporting.

Wear your badge photo-side out and above the waist while on Lab property, including leased spaces. Remove your badge from sight when you leave LANL property and are on public property (e.g., restaurants, grocery store, doctor's office, etc.).

Non-government owned cell phones, PDAs, iPods, MP3 players, Fitbits, and other [portable electronic](#) devices (PEDs) may not be connected to Lab computer systems or introduced into security areas without prior approval.

Bluetooth must be turned off while on Lab property with the exception of the Wellness Center. PEDs are allowed in open areas and most property protection areas. Always be aware of security policies regarding PEDS in limited areas and your proximity to classified work/discussions.

Photography is prohibited on Lab property unless prior authorization has been obtained in accordance with [P217](#).

All Lab employees are subject to random [drug and alcohol testing](#) and [vehicle inspections](#) (government and personal) by the protective force. Random inspections typically last less than five minutes. Briefcases and other personal items (e.g., purses, satchels, boxes) should remain in the vehicle while the search is under way. You will be asked to display the barcode for any Laboratory mobile or PED devices in the vehicle. Generally, barcode labels are placed behind/under the battery or back cover. Barcode labels also may be located on the back of the unit.

Untagged and unattended bags are assumed to be hazardous and may be destroyed. Tag your bags. Click [here](#) for more information. You can usually find tags in the J. R. Oppenheimer Collaboration Space.

You are required to stop at all vehicle access portals (VAPs). VAP controls may change depending on the Lab security condition ([SECON](#)) level, the time of year, holidays, and current events around the world. Information is provided on emergency notification boards around the Lab and through the LANL alert system. Always follow verbal and hand signal direction from a protective force officer.

Parking is not allowed within 20 feet of posted security fences except where parking spaces have been defined by painted lines, parking bumpers or signs. You must notify the protective force at 505-667-4437 if you leave a vehicle on Lab premises overnight outside the Commuter Overnight Parking area adjacent to the TA-3 Transit Center (requires a Commuter Overnight Parking Permit). Click [here](#) for more parking information and requirements.

Tips

Lab-specific

Computer Drives

You will need certain drives the further you are into your position. For example, History Resources for research or Pu_ University for indexing projects. Ask your manager for access. If you can't find a drive you have access to, please ask members on your team for a drive link.

Equipment Certification

If you are on the Digital Collections Team and hear about "equipment certification," you cannot do this until after you are onsite. It is a program to certify hands-on knowledge of NSRC digitization equipment.

Government Vehicles

There are government vehicle(s) available for your group/division. Vehicle sign-out sheet(s) and key(s) are located at TA-03-1400, Room 6106 (PADWP office) or Room 5112 (XCP-DO). Vehicles are available on a first come first serve basis. You may not smoke or use a cell phone while operating a government vehicle, nor may government vehicles be left running while unattended.

Laptop

When working on your LANL laptop, save your work to your specific U drive, not to the laptop. Your U drive will (most likely) be your Z#. If you save to your U drive, you will not lose data if something happens to your laptop.

LA-URs and RASSTI

[RASSTI](#) is the Review and Approval System for Scientific and Technical Information. If you write articles, papers, or anything for wide (or public) release, you will need to go through the RASSTI process. RASSTI assigns:

- LA-UR numbers to unclassified, unrestricted documents intended for public release
- LA-CP numbers to controlled unclassified documents (CUI)

Mail

The mailbox for your physical mail is located in the corridor outside your office pod. If you are working offsite, your default mail stop is A150. The Lab mailing address is:

LANL
P.O. Box 1663
Los Alamos, NM 87545-1663

Nuclear Fundamentals

Within your first several months, you will be assigned [Nuclear Fundamentals](#), Module 1. It is a three-day course. You will be emailed class links about a week before it begins. You may or may not be assigned Nuclear Fundamentals, Module 2. Keep an eye on Utrain for Module 2 to sign yourself up, if need be.

Outlook Calendars

These shared calendars may be of interest:

- WRS events that might be of interest: 03-1400-Shared-weapons_events

Phone Numbers

Because of the secure locations on campus like the NSSB, it's good to write down phone numbers to take with you. Waiting in the NSSB lobby is a bit more comfortable if you have Nanette, Ling, or Chris'

phone numbers in a notebook. If there is a change of plans or an issue, you can call them from the lobby phone. It is a back-up plan instead of having to go back out to your car to retrieve your personal phone.

Indexing and Metadata Standards

You may be assigned an unclassified, remote indexing project. If so, keep in mind that the NSRC is a growing classified library. Universal in-house metadata and indexing standards are developing. Check-in with your supervisor about current standards. Try to provide researchers with the best route(s) to finding information. When in doubt, default to the Library of Congress authority ID for naming conventions.

Remote Desktop

To access a remote desktop on your LANL laptop, go to your computer search bar and type “RDP”. It will open a box that asks for a specific computer number. Input the computer number your supervisor requested you have access to. Press connect.

Timecard

Enter your time each week on your last workday. Vacation hours may be entered ahead; however, productive hours should not be entered ahead. You must obtain pre-approval from your supervisor for vacation leave. Click [here](#) for more about Oracle and Time and Labor (T & L).

Here are your cost codes:

<u>Type:</u> Regular (regular schedule)	Project: ?	Task: ?
ASK YOUR ADMIN for your cost codes		
<u>Type:</u> Holiday (holiday pay up to 8 hours)	Project: V50000	Task: 00000000
<u>Type:</u> Vacation (planned absence)	Project: V50000	Task: 00000000

Cost codes for **Sick**, **Vacation-Sick** (unplanned absence), **LWOP** (leave without pay), and **Report Pay** (Lab or area closure) time are the same as **Holiday** and **Vacation** time, BUT input the correct type. The type refers to where the hours come from. Also, if there is a Lab or area closure, report pay must be approved, which would be indicated by your manager or the Emergency Operations Center (EOC). Cost codes may change and other codes will be provided as projects are initiated.

Time Entry & Work Schedule

Enter your time weekly no later than your last work day. Coordinate time entry with your group timekeeper (Ling Stull) if you know you will not be able to enter your time by the time approval deadline. Reporting deadlines may change due to holidays, snow days, or other special conditions.

Corrections to timecards should be made by the end of the next time reporting period if possible.

If you have permission from your supervisor to swap Fridays, note the change in the comment section of both time cards. You are required to submit hours consistent with your pre-approved working Friday schedule (A or B). Your Friday swap will not be reflected in the hours submitted for that week, only in the comment section. For details, refer to Work Schedules [P761](#).

Requesting Time Off/Sick Leave

If you need to call in sick, leave early due to a non-work related illness, or **request vacation** or sick leave, email wrs-nsrcdc-request@lanl.gov if you are in the NSRC-DC group and wrs-nsrcms-request@lanl.gov

if you are in the NSRC-MS group. This email is forwarded to your group leader and manager. If you do not have access to email, contact your manager or group leader directly. This is important for accountability in the event of an evacuation or emergency at your work location, calls to report for drug testing, family emergencies, etc.

If you experience a non-emergency work related injury or illness (i.e., an event or exposure in the work environment either caused or contributed to the resulting condition or significantly aggravated a pre-existing injury or illness), notify your supervisor ASAP, even if the condition develops after normal work hours. During normal work hours, report to [Occupational Medicine](#) (OccMed) at TA-03-1411. During off hours, contact the on call OccMed provider at 505-667-0660 for direction on where and when to report for evaluation and treatment (if necessary).

For details, refer to Sick leave policy [P730-3](#). To learn more about leave policies, click [here](#).

Receiving an Electronic W-2

You are automatically enrolled in receiving a paper W-2. To receive your W-2 electronically, you must make this selection in Oracle. You will receive an electronic W-2 faster than a paper W-2 mailed to your primary address. To sign up for an electronic W-2, “say NO to paper” via Oracle LANL Worker Self Service → Payroll → Update W-2 Preference.



Further information can be found on the LANLInside [Tax page](#) or by emailing tax@lanl.gov.

Local Life

Commuting

If you take the ([Blue Route](#)) bus from Santa Fe to Los Alamos, factor in extra commute time to walk from the Lab bus stop to your workspace.

If you drive, consider factoring in extra commute time to wait in line at the Vehicle Access Portal as more people return to the Lab from working remotely.

Los Alamos Living

- Google is inconsistent regarding Los Alamos restaurants, hours, and events. Check out local Facebook groups like “Keep it Local Los Alamos.”
- For buying and renting a home, two useful sites are the Facebook Group “Rentals in Los Alamos & White Rock” and Craigslist.

Lastly, please reach out.
We are excited you are here!

1.1 Chapter 1: Personnel Security

1.1.1 Badge Holder Responsibilities

Badges must be worn between the neck and waist with the photo facing out at all times while on Lab owned or leased space. All individuals on Lab property must be badged with a LANL badge, HSPD-12 badge, or a visitor badge. Remove your badge when you leave Lab property. Your badge should not be used as a means of ID for unofficial purposes and it should never be photocopied.

1.1.2 Lost, Forgotten or Stolen Badges

If you suspect or know, your badge was stolen, please call the Security Incident Team (SIT) at 505-665-3505 immediately and report to the Badge Office for a replacement.

If you have lost or forgotten your badge at the start of the workday, please report to the Badge Office to obtain a temporary badge. You will need a driver's license or other form of valid photo ID. Please keep in mind that employees are only allowed two temporary badges within a one-year period. A third temporary badge within a yearlong period will require Group Leader approval. **The temporary badge will be active for 5 working days.**

If you have not found your badge at the end of the five-day period, please report to the Badge Office on the day after the expiration date listed on your badge. You will be asked to fill out Form 1672: Notification of Permanent Inactivation of Badge and you will be given a replacement.

Cleared individuals will receive a LANL site-specific Badge until a new HSPD-12 badge can be reordered. If you find your badge, please immediately return the temporary and the original badge to the Badge Office. A lost badge cannot be re-activated without the temporary.

1.1.3 Generic Badges

Groups that use the generic badges must develop procedures for their control, issue, and recovery prior to obtaining the badges from the Badge Office. Use of these types of badges are limited to the specific building or facility covered by the procedures, and use of these badges outside of these buildings or facilities is prohibited. Organizations who fail to develop and implement procedures will lose the privilege of issuing generic badges.

Escort Required (Orange)



Generic “ESCORT REQUIRED” visitor badges (orange) are usually building-specific and grant short-term escorted access from the **Limited Security Area** boundary to the building identified at the bottom of the badge. Uncleared US visitors must be continuously escorted when using this badge. This badge can be used for escorted access down the Pajarito Corridor given that the building identified on the bottom of the badge is within the Corridor.

Limited Site General Services (Blue)



The Limited Site General Services badge can be used for multiple LANL locations and facilities. Individuals issued this badge must be escorted at all times. This badge is valid for escorting uncleared US citizens in the Pajarito Corridor. An activity security plan is required prior to issuance and must be approved by the Badge Office.

Generic Visitor (Blue)



This Generic visitors badge is used for Property Protection Areas (PPAs) and is building specific. Individuals issued this badge do not need to be escorted unless they will be entering the Pajarito Corridor. Building specific generic badges can be used for entry into the Pajarito Corridor provided the individual is escorted through the vehicle access portal (VAP) and the building identified on the bottom of the badge is located within the Corridor. Once the individual is at their destination they no longer need to be escorted.

Annual Security Refresher

Cleared Employees must complete the Annual Security Refresher (**Course #1425**) once a year in order to maintain access to LANL facilities. **It is the responsibility of the employee to keep track of when to complete this training.** Please be aware you will be locked out of all LANL facilities until the required training is complete and your access has been restored.

Since you have been locked out of LANL facilities you cannot be escorted into property protection or security areas to take the training. The training may be completed at the White Rock Training Center or the Research Library (located just across from the Otowi building).

Reporting Requirements

LANL employees and its subcontract workers have a contractual obligation to promptly report specific conditions affecting the status of an employee or applicant's security clearance. Further, all cleared workers and applicants have a specific obligation to truthfully provide all requested information. If you are a clearance holder and involved in any of the following it must be reported to the Clearance Processing Team via clearance@lanl.gov within one work day of the reportable condition(s):

- Any change in citizenship status;
- Legal action effected for a name change;
- Any use of an illegal drug, or use of a legal drug in a manner that deviates from approved medical direction;
- Any arrests, criminal charges (including charges that are dismissed), citations, tickets, summons, or detentions by Federal, State, or other law enforcement authorities (including Tribal authorities) for violations of law within or outside of the U.S. Traffic violations for which a fine of up to \$300 was imposed need not be reported, unless the violation was alcohol- or drug-related;
- An immediate family member assuming residence in a sensitive country;
- Hospitalization for mental health reasons or treatment for drug or alcohol abuse;
- Employment by, representation of, or other business-related association with a foreign or foreign-owned interest or non-U.S. citizen or other individual who is both a US citizen and a citizen of a foreign country;
- Personal or business-related filing for bankruptcy;
- Garnishment of wages;
- Any situations or incidents that may have the tendency to impact a worker's eligibility for a security clearance.
- When a cleared worker or applicant no longer requires access to classified information or special nuclear material.
- When a cleared worker or applicant is transferred to another location internal or external to LANL.

Cohabitation

Under separate reporting timeline criteria listed above, provide a completed DOE F 5631.34, *Data Report on Spouse/Cohabitant* to clearance@lanl.gov, within forty-five (45) days of marriage or cohabitation. *Note: A cohabitant is a person who lives with the cleared worker in a spouse-like relationship or with a similar bond of affection or obligation but is not the individual's legal spouse, child, or other relative (in-laws, mother, father, brother, sister, etc.).* Each clearance holder/applicant requires reporting whether the cohabitant is cleared or uncleared. A new form will need to be completed if the status changes from a cohabitant to a spouse.

Drug/alcohol testing

As a Department of Energy (DOE) laboratory with a national security mission, Los Alamos National Laboratory cannot tolerate illegal activity and must ensure a work environment that is free from unauthorized or illegal use, possession, or distribution of alcohol or controlled substances.

Testing of workers, including subcontractors, for drugs and alcohol is conducted under the following circumstances:

- Random Basis
- Reasonable Suspicion
- Post-Accident
- Post-Incident
- Testing related to applying for or holding a clearance
- Follow-up testing
- Special Access Programs (DOT, HRP)

Marijuana has been legalized in some states; however, it remains a controlled substance under federal law. Our Laboratory is a federal institution and a positive drug test at the Lab, including for marijuana, is a termination level offense. Employees should be aware of the following possible situations:

Legalization in other states:

- Ingesting marijuana in a state where it is legalized is not a valid excuse for a failed drug test.

Medical marijuana:

- The Laboratory does not recognize medical marijuana. A medical marijuana card is not an excuse for a failed drug test.

Edible products:

- There are now many edible products containing marijuana. Accidental ingestion is not an excuse for a positive drug test, unless the employee self-reports the accidental ingestion *prior* to being called for a drug test.

In cases of unwitting ingestion the Laboratory will consider credible evidence that the employee truly was unaware that he or she had ingested the drug. Employees must be vigilant to ensure they avoid ingesting illegal drug, even by accident. Drug and alcohol testing can be requested during work hours by calling Personnel Security at 505-665-7866. After hours requests can be made by calling 505-667-8378 (P-TEST)

1.2 Chapter 2: Physical Security

1.2.1 Security Areas

It is important to know where you are at the Lab. Are you in an area where classified information or special nuclear materials can be discussed and handled? Physical protection measures designate the type of Security Area and activities that can take place within that area. The following areas are designated as security areas at the Laboratory:

General Access Areas (GAAs)

GAAs are accessible to all workers and the public.

Examples include: Otowi Cafeteria or the first floor of the J. Robert Oppenheimer Library.

Badges are not required for individuals in GAAs.

Access controls such as badge readers or LANL keys are not required for entry. Classified activities or special nuclear material cannot be discussed or stored in a GAA.

Property Protection Areas (PPAs)

PPAs are established to protect workers, buildings, facilities, and property.

Badges are required for individuals in PPAs.

Typically, PPAs are equipped with an Apollo badge reader that requires only a badge swipe for entry or a LANL key.

Uncleared and Q/L are permitted to enter area without being escorted. Classified activities or special nuclear material cannot be discussed or stored in a PPA.

Limited Areas (LA)

LAs are Security Areas established for the protection of classified matter and/or

Category III SNM

Badges are required for individuals in a LA.

LAs are equipped with Argus badge readers that require a badge swipe and a PIN for entry.

Q/L cleared are permitted. Uncleared must be properly escorted into the LA. Classified activities and Category III special nuclear material may be discussed or stored in a LA.

Q-Only Limited Areas (LANL-specific)

Q cleared only Limited Areas allow access to only Q cleared individuals.

Uncleared/L-cleared must be escorted in these areas.

Buildings, such as the NSSB, are posted at the entrances that they are Q-cleared only.

Badges are required for Q cleared only areas.

Q cleared only areas are equipped with Argus badge readers that require a badge swipe and PIN for entry.

Classified activities and Category III special nuclear material may be discussed or stored in Q cleared only areas.

Sensitive Compartmented Information Facility (SCIF) and Special Access Program Facility (SAPF)

SCIFs/SAPs require additional security measures for entry. It is best to contact the Sensitive and Special Operations (SSO) for guidance and requirements.

Protected Areas (PAs) – TA-55

Badges are required for individuals in the PA.

Additional approvals and training are required for unescorted access into the PA.

Q/L are permitted. Uncleared must be escorted.

The PA is equipped with personnel protective identification and verification booths (PPIV). It is essentially equipped with an Argus badge reader that requires a badge swipe, PIN, and hand geometry. The booths are also equipped with metal detectors. PAs are Security Areas established to protect Category II SNM and classified matter. PAs may also be established to provide a concentric security zone surrounding an MAA.

Material Access Areas (MAAs) TA-55, PF-4

Badges are required for individuals in the MAA.

Additional approvals and training are required for unescorted access into the MAA.

Q cleared are permitted. Uncleared and L cleared must be escorted. The MAA is equipped with personnel protective identification and verification booths (PPIV). It is essentially equipped with an Argus badge reader that requires a badge swipe, PIN, and hand geometry. The booths are also equipped with metal detectors.

Material Access Areas are Security Areas established to protect Category I SNM and Category II SNM with credible rollup to Category I.

Vaults and Vault-Type Rooms (VTRs) are subject to additional requirements.

The escort will inform the visitor that prohibited and controlled articles are not permitted in the V/VTR.

When the V/VTR visitor enters and exits the V/VTR, V/VTR Escorts must check the V/VTR visitor's carried belongings for unauthorized controlled and prohibited items. The visitor will verbally confirm that he or she is not introducing prohibited or controlled articles into the V/VTR.

Processing, discussing, and storing classified matter is only allowed in Security Areas (LAs and higher).

1.2.2 *Prohibited/Controlled Articles*

Prohibited Articles

The following prohibited articles must not be brought on Lab property unless specifically authorized:

- Nongovernment-owned firearms.
- Dangerous weapons and explosives (including dangerous instruments or materials likely to cause substantial injury or damage to persons or property). Includes pocket, hunting, or other sharp knives with blades longer than **2.5 inches**. (Note: This requirement does not prohibit workers from possessing knives for official Lab work or fixed blade knives with a blade length longer than 2.5 inches that are to be used in the preparation of food (such as steak knives or cooking knives).
- Alcoholic beverages.

- Controlled substances (for example, illegal drugs and associated paraphernalia, but not prescription medication).
- Items prohibited by local, state, or federal law.

The Protective Force or the Los Alamos Police Department may confiscate unauthorized prohibited articles on Laboratory property.

Controlled Articles

A controlled article is a non-LANL owned device that can store, read, write, record, or transmit data. These items are **not allowed in Security Areas and are not allowed to be plugged into LANL systems** regardless if the system is located in a Security Area or not. Under certain circumstances, controlled articles may be approved for use in Security Areas by completing Form 1897.

Controlled articles include:

- Cameras
- Cell phones and smart phones
- Personal Digital Assistants (PDAs)
- Digital audio players
- Laptop or tablet computers
- Recording equipment
- Medical devices, ankle monitor bracelets
- Copiers and/or scanners with a hard drive and portable scanners
- Two-way pagers
- Two-way radios
- Compact Disc/Digital Video Disc (CD/DVD) write drive
- External hard drive
- Flash memory
- Universal Serial Bus (USB) memory device (i.e., thumb drive, memory stick, jump drive)

Refer to the Controlled Articles Procedure (P217) for the complete requirements.

Escorting

Escorting in Security Areas is allowed for valid, official purposes. The Host must establish the need for escorted work by verifying:

- The work is official LANL business that can be accomplished only in the security area.
- The work cannot be provided by a worker who has the required clearance level or access authorization for unescorted access to the area.

Reasons that are not valid for escorting:

- Activities of purely social nature (e.g., retirement parties, birthday celebrations) except for official Lab events.
- Spouses/children/friends that are not employed by LANL cannot attend social functions on Lab property (unless it is an official Lab event e.g. Family Days).
- Allowing uncleared US citizens known to have a suspended, revoked, or denied DOE security clearance access to a Security Area.

- Foreign nationals, unless there is prior approval on Form 982. Additional forms are required for foreign national access to a security area.

Property Protection Areas (PPAs) and Other Security Areas:

Minor visitors are generally not permitted in PPAs and other Security areas. Minor visits must be approved by the respective Division Leader prior to the visit for the following:

- Official Lab-sponsored events, such as family day
- Special activities with an educational purpose, such as school field trips or job interviews.

Escorts must:

- Determine the need for the escorted activity;
- Be eligible to escort (take the Escort Training and be cleared for the area to be visited);
- Coordinate with workers in the site to be visited; and know site-specific requirements.
- Acquire the necessary badge for the visitor if necessary (e.g., visitor badge);
- Brief the visitor about prohibited and controlled articles, security, safety, emergency procedures, and other site-specific requirements; Notify those in the area about the presence of a visitor.
- Not exceed the escorting ratio of **five visitors per escort**;
- Ensure visitor is wearing the appropriate badge visibly;
- Maintain visual and/or aural control of the visitor;
- Protect classified material; and
- Hand off the visitor to a qualified escort if needed.
- Retrieve and return visitor badges; and

The escort ratio at LANL is **one-to-five escort-to-visitor**. The one-to-five escort-to visitor ratio unless stated differently in an Activity Security Plan.

Escorts must complete Lab escort training (course #18366) before conducting escorting activities.

1.2.3 *Tag Your Bag*

Untagged bags left in public places at the Lab are assumed hazardous devices and are treated as such. Place ID tags on all types of bags - backpacks, duffel bags, lunch boxes, computer (laptop) cases, fanny packs, and purses that you bring on Lab property. Proper ID is essential to keeping your belongings in one piece. To avoid the possibility of having your lunch, laptop, or important documents destroyed, ensure you have an ID tag on your bag. For write-on bag tags, contact the LANL Badge Office or your WSST representative.

1.2.4 *Piggybacking (Vouching)*

Piggybacking (letting someone follow through an access control system) and **tailgating** (following someone through an access control system without the knowledge of that person) are never allowed in areas where an active badge reader system controls access. The individual opening the door/gate is responsible for ensuring that it latches properly and piggybacking or tailgating do not occur.

Access control systems such as badge readers that are used to operate gates and/or doors exist for reasons besides preventing outsiders from gaining access to Laboratory areas. A person may have an expired badge, may be delinquent in their security training, may have had their clearance downgraded or revoked, or may have been fired from the Lab. Piggybacking and/or tailgating violations should be reported to the Security Incident Team.

Contact your Deployed Security Officer (DSO) or SEC-PSS for more information or refer to Security Areas, Property Protection Areas, and General Access Areas (P202-1).

NOTE: Inoperative badge readers are NOT considered active badge readers. Owning organizations can implement manual badge checks performed by a DSO, a properly cleared employee or Protective Force personnel until the badge reader can be repaired.

1.2.5 *Emergency Responders*

Each 911 emergency occurs under a unique set of circumstances. Emergency Responders, such as Los Alamos Police Department personnel, must respond and have full access to all LANL property. LANL building occupants must provide immediate access to responding officers on a 911 emergency call. It is the duty of the officer responding to a 911 call to “clear” the situation and ensure that everyone in the building is safe and that no additional police/medical response is needed.

1.2.6 *Photography*

The use of photographic equipment on Laboratory property is prohibited without approval. Workers who need to take photographs with a camera must:

- Request prior approval by submitting Form 1897PA

The worker who will use the photographic equipment must fill out Form 1897PA, Photographic Equipment and Activity Authorization, now available for electronic submission. Form 1897PA must be reviewed and authorized by the worker’s responsible line manager

- Carry a copy of the approved 1897PA while taking photographs
- Present the approved 1897PA to anyone who requests to see it.

Workers who see photography on Laboratory property should:

- Question anyone taking pictures
- Ask to see the photographer’s approved Form 1897PA
- Report any unauthorized photography immediately by contacting the protective force at 505-667-4437 or the Security Inquiry Team at 505-665-3505.

Photographic equipment installed for facility surveillance, installed in an experimental apparatus, or otherwise incorporated into a system or apparatus used for programmatic work are exempt from the authorization requirements. Workers should contact the Physical Security Team for guidance.

LANL issued smart phones with enabled camera capabilities are authorized for use at LANL.

1.2.7 *Protective Force Operations*

Protective Force Operations (SEC-PFO) personnel are comprised of Subject Matter Experts (SMEs) that perform a variety of day-to-day operations monitoring of the LANL Protective Force organization. The Protective Force Operations Group oversees the Protective Force (C-LA) and the following security services:

- Canine Support
- Post 10/Inspection Station
- Protester Activity/Public Demonstration Permits
- Special Events Management

- Protective Force Staffing Requests at TA-55 and Other LANL Areas

1.2.8 *SECON Levels*

The Defense Security Program (DFS) implements different access control requirements for Vehicle Access Portals (VAPs) depending on the security condition (SECON) the Lab is in at any time.

The Security Conditions (SECONs) system describes a progressive level of common sense protective measures that may be implemented in response to a malevolent or terrorist threat to any or all DOE facilities, assets, and personnel. The purpose of the SECON system is to establish standardized protective measures for a wide range of threats and to help disseminate appropriate, timely, and standardized information for the coordination and support of DOE crisis or contingency activities. Once one of the five SECON levels is declared, the associated protective measures should be implemented, to the extent they apply to the individual site or facility, as soon as possible.

A description of each SECON level is outlined below.

SECON 1, Severe Condition - This reflects a severe risk of terrorist attacks. This condition applies in the immediate area where a malevolent or terrorist attack has occurred that may affect the site or when an attack is initiated on the site.

SECON 2, High Condition - This condition is declared when there is a high risk of terrorist attacks. This condition applies when an incident occurs or intelligence information is received indicating that some form of malevolent or terrorist action against personnel and facilities is imminent.

SECON 3, Elevated Condition - This condition is declared when there is a significant risk of terrorist attack. SECON 3 applies when an increased and more predictable threat of malevolent or terrorist activity exists.

1.2.9 *Inspections*

All vehicles passing through Vehicle Access Portals are subject to inspection.

Inspection Process:

A Protective Force officer will notify a driver to pull over to a search area, which is marked with a sign and set off with traffic control devices.

An inspection team, which includes a canine team, will inspect the entire vehicle (under the hood and chassis, the inside, and any items that are towed behind or secured to the roof of the vehicle).

If your vehicle is chosen to be inspected, follow the directions of the Protective Force officer. You will be required to open all accessible compartments on the vehicle.

Upon completion of the inspection, the team will either give the driver permission to proceed or secure the vehicle and the surrounding area as necessary.

Workers must cooperate with and follow the instructions of the Protective Force during inspections. Failure to do so may result in a security incident and notification of the Security Inquiry Team and the worker's line management

Explosive Detection Canine Patrols

The parking areas or structures at the Laboratory have explosive detection canine patrols. If a canine detects a threat, the Protective Force as necessary will re-route traffic or cordon off the area until an explosives team determines it is safe for re-entry.

1.2.10 *Post 10*

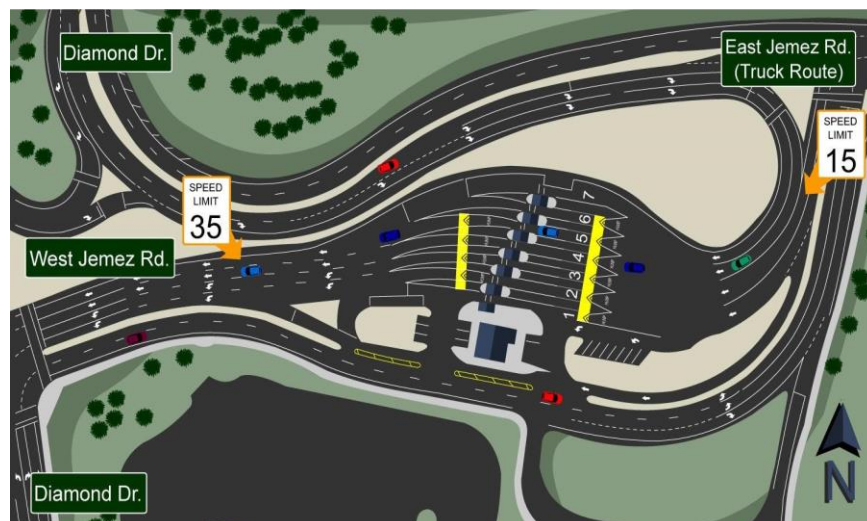
Drivers of all non-government commercial delivery trucks, privately owned RVs, large vehicles, etc. must stop at Post 10 for truck inspections. Drivers will then need to present time-stamped inspection passes from Post 10 to Protective Force officers stationed at the VAP.



1.2.11 *Vehicle Access Portals (VAPs)*

All vehicles entering LANL property are required to stop at the East and West Jemez Road VAPs for vehicle checks. Drivers must show picture identification (DOE or federal badge or valid driver's license) before proceeding at the direction of Protective Force officers.

East Jemez VAP (VAP 6)



Traffic Lanes 1: Closed except for emergencies and maintenance operations.

Traffic Lanes 2-7: Drivers are required to stop and present LANL badges or a valid form of government identification to Protective Force officers, drivers may proceed upon direction of officers.

Commercial delivery vehicle drivers must also present their inspection passes from Post 10. All vehicles (commercial, private, government) are subject to random inspections while on Lab property.

Non-work Hours: Vehicles entering LANL at the East Jemez VAPs during non-work hours (between 7 p.m. and 5 a.m. during the weekdays and all-day on weekends) will be funneled into the center lane. Drivers are required to stop at the center lane and present a LANL badge or a valid form of government identification to Protective Force officers. All other VAP lanes will be closed during non-work hours

West Jemez VAP (VAP 4)



Traffic Lane 1: Closed except for random inspections.

Traffic Lane 2: Drivers are required to stop and present LANL badges or a valid form of government identification to Protective Force officers. Drivers may proceed upon direction of officers.

Commercial delivery vehicles must present inspection passes from Post 10. All vehicles (commercial, private, government) on Lab property are subject to random inspections.

Pajarito Corridor

The Pajarito Corridor is open to badge holders only. Unbadged drivers and passengers, including minors, are prohibited from traversing the Pajarito Corridor in the cars of badged workers.

Pajarito Corridor VAPS (VAP 15 and 18)



All Lanes: Pajarito corridor is open to badge holders only. Drivers are required to stop and present LANL badges to Protective Force officers, drivers may proceed upon direction of officers.

Commercial delivery vehicle drivers must also present their inspection passes from Post 10. All vehicles (commercial, private, government) are subject to random inspections while on Lab property.

1.3 Chapter 3 Safeguards

1.3.1 Information Security

Access Authorization/Clearance levels

Access Authorization is an administrative determination made by DOE that an individual is eligible for access to classified information in accordance with 10 CFR 710, *General Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Special Nuclear Material*.

No individual will be provided access to classified information or SNM unless that individual has been granted the appropriate Access Authorization and possesses a need-to-know. Access to, knowledge of, or possession of classified information or SNM will not be afforded to any individual solely by virtue of the individual's office, position, or security clearance.

Q Access Authorization is required when the duties of the position require access to any of the following:

- Top Secret Restricted Data (TSRD)
- Secret Restricted Data (SRD)
- Category I, II, & III Special Nuclear Material (SNM)
- Top Secret/National Security Information (TSNSI)
- Top Secret/Formerly Restricted Data (TSFRD)

L access authorization is required when the duties of the position require access to any of the following:

- Confidential Restricted Data (CRD)
- Category II & III Special Nuclear Material (SNM)
- Secret/National Security Information (SNSI)
- Confidential/National Security Information (CNSI)
- Secret/Formerly Restricted Data (SFRD)
- Confidential/Formerly Restricted Data (CFRD)

Clearance Requirements for Access to Classified Matter		
Category and Level of Classified Matter	Q cleared	L cleared
Confidential National Security Information	Permitted	Permitted
Confidential Formerly Restricted Data	Permitted	Permitted
Confidential Restricted Data	Permitted	Permitted
Secret National Security Information	Permitted	Permitted
Secret Formerly Restricted Data	Permitted	Permitted
Secret Restricted Data	Permitted	Excluded
Top Secret National Security Information	Permitted	Excluded
Top Secret Formerly Restricted Data	Permitted	Excluded
Top Secret Restricted Data	Permitted	Excluded

Need-To-Know (NTK)

Need-to-know is defined as a determination made by workers having responsibility for classified or sensitive information or matter that a proposed recipient's access to such classified or sensitive information or matter is necessary in the performance of his or her official or contractual duties of employment.

Determining Need-to-Know

Any worker who has been granted access to classified matter must determine another worker's clearance and need-to-know before granting access to that matter. Need-to-know must be established by determining what matter will be accessed and determining that the recipient requires access to

this matter to perform his or her official duties through current relationships, tasks, duties, and assignments or confirmation by an RLM.

Incidental access may be granted to individuals (such as audits by LANL employees or external organizations) who handle or come into contact with classified matter but whose job functions do not include review or other use of the classified matter.

Note: The worker having responsibility for the information determines need-to-know. In some cases (such as audits by external organizations), need-to-know may be determined by LANL senior management or other government agency rather than the worker responsible for the information.

Controlled Unclassified Information (CUI)

The following are types of Controlled Unclassified Information (CUI) that are required to be protected:

Naval Nuclear Propulsion Information

Documents may be designated U-NNPI if they contain unclassified information concerning any aspect of the propulsion plants of naval nuclear-powered ships and prototypes, including associated nuclear support facilities. Some NNPI is classified. UNNPI is considered CUI.

Official Use Only (OUO)

To be designated DOE OUO information, the information must have the following characteristics:

OUO is Unclassified and has the potential to damage governmental, commercial, or private interests if disseminated to any person who does not have an NTK the information to perform their jobs or other DOE-authorized activities

Justification to protect the information is described by at least one of seven Freedom of Information Act (FOIA) exemptions: Exemptions 3 through nine.

Export Control Information (ECI)

ECI is unclassified technical information, which is subject to export control statutes and regulations, and for which unrestricted public dissemination could aid potential adversaries of the United States.

Unclassified Controlled Nuclear Information (UCNI)

UCNI is certain unclassified information about nuclear facilities and nuclear weapons that must be controlled because its unauthorized release could have a significant adverse effect on the national security or public health and safety. The voice transmission of UCNI over open phone lines is prohibited, per 10 CFR 1017, Subpart E, and Physical Protection Requirements for Unclassified Controlled Nuclear Information (pdf). A Secure Terminal Equipment (STE) line is required for UCNI phone conversations at LANL.

Storage, and Reproduction of CUI

All CUI information shall be stored in a locked room or locked receptacle (e.g. desk, file cabinet, safe). CUI information stored on a computer shall meet all LANL password, authentication, encryption, or file access control requirements to protect the files from unauthorized access.

All copies of CUI (including 3-D print prototypes) must be protected, accessed, stored, marked, transmitted, and destroyed in the same manner as the originals.

Destruction of CUI

All non-electronic CUI documents must be destroyed by any means that prevents the retrieval or export of the information.

CUI material may be destroyed by shredding it in an approved shredder, or use of a burn box approved for unclassified matter.

Other methods may be used to destroy CUI material if they are reviewed and approved by a Subject Matter Expert (SME). Workers must contact their deployed security officer for assistance if alternative destruction methods are needed.

The requirements for handling CUI can be found in P204-1.

Classified Information

Access to classified matter must be limited to workers who possess the appropriate access authorization (i.e., security clearance), relevant access approvals (i.e., Sigma authorities, SCI clearance, etc.) and who have a need-to-know for the performance of official duties.

All individuals who are authorized for access to classified information must receive instruction with respect to their specific security duties as necessary to ensure that they are knowledgeable about their responsibilities and applicable requirements.

Prior to classification review, information that may be classified must be protected at the highest potential classification level and category of the information it contains.

The originator must ensure that a derivative or original classifier reviews the information and determines its classification including:

- When unsure of the classification level or category of a draft or working paper and for all final products that may contain classified information.
- The originator must ensure that all classified matter is appropriately marked according to the classification determination.
- Each area where classified matter is processed, handled, or stored must employ need to-know controls, appropriate physical security, and access control measures to detect unauthorized physical, visual, and aural access.

Hand-Carrying Classified Matter Between Security Areas

Prepare a classified matter receipt if the matter is accountable.

Packaging the Classified Matter

An appropriate cover sheet **must** be used to protect the contents from view while the document is being transported. The classified matter **must** be protected by either:

Using an envelope:

- Place the covered document in an opaque envelope.
- Address the envelope with the sender's name, group, and classified mail stop on the upper left of the envelope and the recipient's name, group, and classified mail stop in the center of the front of the envelope.
- Seal the gummed flap of the envelope.

Using a briefcase:

- Place the covered document in a locked briefcase.
- Mark the briefcase with the name, group, and classified mail stop of the person carrying the case.

Reusable fabric bags with key locks (not bank/money bags) are permitted for hand-carrying classified matter on LANL property. Fabric bags used to transport classified matter **must** remain closed when in the locked position.

Transporting the Matter within LANL Security Areas

Classified matter **must** be hand-carried directly from one LANL Security Area to another Security Area.

Classified matter **must** be delivered to a worker with required clearance and need-to-know or placed in an approved storage container. Workers hand-carrying classified matter **must**:

- Have the required access authorization or clearance level for the information.
- Be aware they are carrying classified matter so it can be protected and controlled.
- Travel directly to the recipient's location without making any stops. (Do not stop in the restroom, a private residence, a restaurant, the Otowi cafeteria, any other LANL office located in an open area, etc.)
- Verify the recipient's clearance and need-to-know before transferring classified matter.
- Inform the recipient that the document is classified and cannot be left unattended.
- Ensure the recipient signs and dates the receipt, if required.

Hand-Carrying Classified Matter Outside LANL

Important! Hand-carrying classified matter outside LANL is permitted only with a contingency plan for delayed arrival and an approved LANL Form 1658, *Certification and Approval to Hand Carry Classified Matter Off-Site*. A contingency plan **must** be prepared by the hand-carrier and approved by the hand-carrier's RLM for each instance of hand-carrying outside LANL. Contact your Deployed Security Officer (DSO) or Security Program Lead (SPL) for assistance in developing a contingency plan. LANL Form 1658 and the contingency plan **must** be submitted to the CMPC Team before departure on travel.

A classified matter receipt **must** be prepared in accordance with the requirements in if the matter is accountable or classified at the Secret level.

Classified matter **must** be properly marked and double-wrapped in opaque material. A locked briefcase **cannot** serve as an outer wrapper when traveling aboard public transportation, but can be used in carrying the double-wrapped package.

Reusable fabric bags with key locks **must not** be used for hand-carrying classified matter outside of LANL.

Classified matter **must not** be removed from approved storage facilities to private residences or other unapproved places such as hotel or motel rooms.

Refer to LANL Form 1658, *Certification and Approval to Hand Carry Classified Matter Off-Site*, for additional requirements.

Destruction of Classified Information

Classified matter must be destroyed using only approved destruction equipment located within an LA or higher Security Area.

Classified matter must be destroyed beyond recognition and must not permit subsequent recovery of classified information.

Acceptable methods for destroying classified matter include shredding, pulping, melting, mutilation, chemical decomposition, or pulverizing.

Destruction equipment **must not** be used to destroy classified matter until approval is granted by the CMPC Team. Approval sticker will be affixed to approve shredders signed and dated.



Electronic storage media containing classified information must be destroyed in accordance with DOE cyber security directives.

Derivative Classifier

Any employee, which includes subcontractor employees, students, managers, etc., who originates a document or other matter in a potentially classified subject area must ensure that a classification review is obtained by referring it to a Derivative Classifier (DC) for evaluation. Employees must complete information security training and understand their responsibilities regarding access to and

handling of classified information, as well review requirements for various work products and publications. P204-3-Classification of Matter, P 204-2-Classified Matter Protection and Control Handbook, and PD1022- Review and Release of Scientific and Technical Information (STI) are several relevant LANL Policy documents that provide further information.

Derivative classification is the process of determining whether information classified under the Atomic Energy Act or determined to be classified by an original classifier is revealed by documents or material under review by the derivative classifier.

Department of Energy Order 475.2B specifies the requirements for the Laboratory's Derivative Classifier (DC) Program. The Classification Group relies on volunteer subject matter experts from groups across the Laboratory to serve as the “first line of defense” in identifying classified information as it is generated.

Emergency Procedures and Protective Actions

Workers must immediately report an emergency as soon as it is safe to do so. Any on-scene observer/worker who is knowledgeable of the incident must make initial emergency reporting promptly, accurately, and effectively.

Call 911 and follow instructions provided by the operator.

Provide a description of the emergency, location, alarms, injuries, and protective actions taken to the 911 operator. Explain what the alarms mean and any related hazards.

Limit the use of acronyms and report the location of the emergency using the Technical Area (TA) and building number. Include the room number and area of the building using cardinal directions if applicable (e.g., TA-03, Building 261, Room A-109, southeast corner of the Otowi building).

Call the LANL EOSC at 505-667-2400 and follow instructions provided by the operators.

Provide a description of the emergency, location, alarms, injuries, and protective actions taken to the EOSC operator. Explain what the alarms mean and any related hazards.

Protective Actions

During any emergency, remain calm and follow instructions from the emergency responders. If safe to do so, always place your work in a safe and/or secure configuration (e.g., machines, tools, glove boxes, hoods). These protective actions will NOT take the place of common sense or of direction provided by the Incident Commander (IC), facility operations center, EOSC, or emergency responders during an emergency incident. Workers are expected to make safe, secure, and responsible decisions when taking protective actions.

Understanding what protective actions to take during an emergency, and if sent an emergency notification, is paramount to safety and survival during an emergency event.

The four protective actions used at LANL are:

- **Evacuation:** A building is evacuated to avoid hazards, such as a chemical spill or fire.

- **Shelter in Place:** This is directed when there has been an airborne release of hazardous materials and the safest option is to shelter indoors until the hazardous plume passes and/or dissipates.
- **Remain Indoors:** Workers will be directed to remain indoors for situations such as severe weather or wildlife in the area.
- **Lockdown:** This term is used for active threat situations (e.g., active shooter) and indicates the need to run, hide, or fight based upon your situation and proximity to the threat.

1.3.2 *Deployed Security*

The LANL Deployed Security program provides deployed security professionals across the laboratory to support a diverse set of customers and critical missions in support of the vital national security mission. Deployed security assists line managers with integrating safeguards and security policies and procedures into daily line functions, and supports key elements of security based on customer work.

Deployed Security Officer (DSO) or Security Program Lead (SPL)

Workers must immediately report any known or potential incident of security concern to a DSO or SPL, and their Responsible Line Manager (RLM).

If, during normal hours of operation, the DSO or SPL cannot be contacted, the worker must immediately notify the SIT directly or contact another DSO or SPL.

If the incident is discovered outside of normal hours of operation, the worker must immediately notify the On Call Duty officer (OCDO). The worker may also notify the DSO or SPL as soon as possible the next business day.

1.3.3 *Security Incidents and Occurrence Investigations*

SIT team

The goal of each inquiry is to determine if a security compromise occurred and whether national security was at risk or damaged. Every inquiry also identifies causal factors for recommended improvements.

Incidents of security concern are actions, inactions, or events that:

- Pose threats to national security interests and/or critical DOE assets;
- Create potentially serious or dangerous security situations;
- Potentially endanger the health and safety of the workforce or public (excluding safety-related items);
- Degrade the effectiveness of the Security and Safeguards (S&S) program; or
- Adversely impact the ability of organizations to protect DOE S&S interests.

Some examples of situations you should report to the SIT include:

- Suspicious email
 - Forward the email to phish@lanl.gov. The SIT staff will determine the risk of the email and a course of action.
- A lost or stolen badge.
- Threats, workplace violence, or harassing phone calls.
- A LANL worker discovers an unauthorized person in a Security Area.

The SIT conducts inquiries to ascertain facts surrounding each incident. The SIT further manages the reporting process of incidents.

LANL's Investigative Services Team (LIST)

The LIST provides investigators who are independent and qualified. Results of the team's inquiries are:

- Conducted in accordance with Lab policies and procedures.
- Communicated to managers for mitigation and corrective actions when they identify internal control weaknesses in Lab processes; and provide recommendations to prevent recurrence of fraud, waste, abuse and theft of government property.

The team is comprised of security professionals that are responsible for coordinating efforts with local, state, and federal law enforcement agencies as necessary.

The Laboratory Investigative Services Team (LIST), in conjunction with the Protective Force and the Los Alamos Police Department, administers the enforcement of parking regulations at the Lab.

1.3.4 End-of-Day Checks

End-of-day checks – as a safeguard – serve as a catalyst for ensuring the following remain intact at the end of each work day:

1. Safety – Life Safety and Welfare Check of Colleagues;
2. Security – Classified Matter Is Stored – No Classified Matter Left Unattended;
3. Security – Red Net Computer Screen Is Locked or Red System Powered Down;
4. Security – GSA Safe Is Locked.

The following guidance is for personnel performing end-of-day checks within the NSSB SALA.

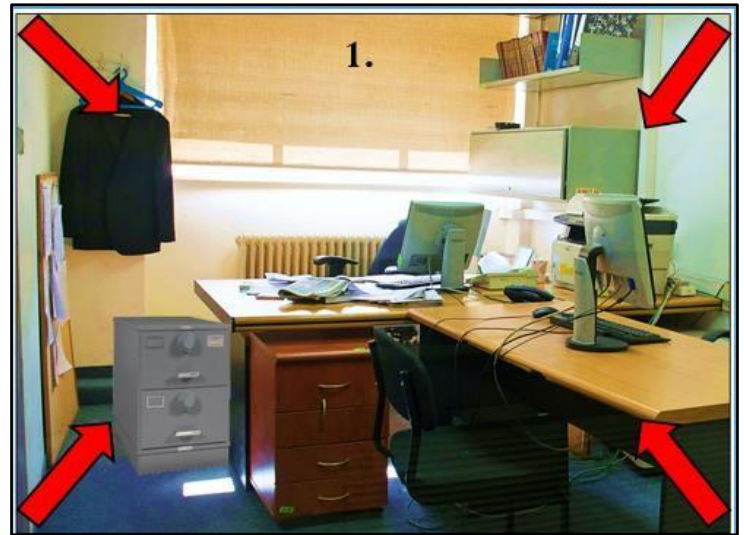
1. SAFETY – LIFE SAFETY AND WELFARE CHECK OF COLLEAGUES: –

After knocking – perform a cursory search of the office to ensure the office occupant is not in need of assistance. If a colleague is in need of medical assistance:

LANL Emergency Operations Support Center (EOSC) is the 24/7 primary point of contact for reporting of LANL emergency incidents **after** calling 911 and notifications of non-emergency incidents.

Note: Dialing 911 from LANL landline telephones connects to a local public safety dispatch center, which uses enhanced 911 (E911) services to identify the physical location of the caller. Ensure the 911 operator knows you are at Los Alamos National Laboratory. IF unsure, THEN call the EOSC (7-2400) and they will direct you to the appropriate resources.

LANL Incident Reporting and Notifications		
Description	Contact(s)	Phone Number
<p>All emergency and non-emergency incidents that could impact worker health and safety. Examples include:</p> <ul style="list-style-type: none"> • Fires or smoke odor • Hazardous material release (actual or suspected) • Abnormal events impacting worker safety and health • Suspicious packages or bomb threats • Suspicious vehicles or persons 	<p>Emergency Operations Support Center (EOSC)</p> <p>Note: EOSC will make additional notifications to the Protective Force, Los Alamos Police Department, Los Alamos Fire Department, and other agencies, as needed.</p>	<p>EMERGENCY DIAL 911 FOR POLICE MEDICAL</p> <p>Then Dial: (505) 667-6211</p>



2. SECURITY – CLASSIFIED MATTER IS STORED – NO CLASSIFIED MATTER LEFT UNATTENDED:

Glance at table/desktop – and surrounding areas – ensuring no classified documents &/or classified removable electronic media (CREM) are left unattended.

If discovered – immediately take possession of the classified matter; call your RLM and DSO.

If you are the owner of a GSA safe, place the classified matter in your safe until the DSO can take possession of the classified matter (typically the next work day).



3. SECURITY – RED NET COMPUTER SCREEN IS LOCKED OR RED SYSTEM POWERED DOWN: –

Locate red net computer; tap on keyboard, ensuring lock screen appears. If the computer screen is not locked – and contents appear to be accessible – lock the screen; or, power down the red system.

Contact your RLM and DSO to report.



4. *SECURITY – GSA SAFE IS LOCKED: –*

Locate the GSA safe –



- First: Attempt to open other drawer(s) by tugging on drawer handle(s) while pressing in button.
- Next: Attempt to open door/drawer with combination dial by turning and pulling on the handle.
- Then: Spin the combination dial three (3) rotations to the left, & stop.



When you have verified that the GSA safe is locked and secure, locate the 702 form – date, initial, and annotate time of-completion.

What if...

1. You come upon a safe that is open (drawer[s] left open)

Lock the safe; date, time, and initial on 702; contact your RLM and DSO to report.

Example 1:

(Safe not opened during work hours)

Before end-of-day check –

STORAGE CONTAINER CHECK SHEET									
From	Room No.	Building	Container No.	Certification					
	111A	3-100	123456	I certify, by my initials below, that I have opened, closed, or checked this storage container in accordance with pertinent agency regulations and operating instructions.					
Month/Year July 2013									
Date	Opened By Initials Time	Closed By Initials Time	Checked By Initials Time	Checked By (If required) Initials Time					
3/7	DN 8:30	DN 8:40	CF 5:03						

After end-of-day check –

STORAGE CONTAINER CHECK SHEET									
From	Room No.	Building	Container No.	Certification					
	111A	3-100	123456	I certify, by my initials below, that I have opened, closed, or checked this storage container in accordance with pertinent agency regulations and operating instructions.					
Month/Year July 2013									
Date	Opened By Initials Time	Closed By Initials Time	Checked By Initials Time	Checked By (If required) Initials Time					
3/7	DN 8:30	DN 8:40	CF 5:03						
3/8	NA			RV 5:27					

Example 2:

(Safe opened and closed – pending end-of-day check)

Before end-of-day check –

STORAGE CONTAINER CHECK SHEET									
From	Room No.	Building	Container No.	Certification					
	111A	3-100	123456	I certify, by my initials below, that I have opened, closed, or checked this storage container in accordance with pertinent agency regulations and operating instructions.					
Month/Year July 2013									
Date	Opened By Initials Time	Closed By Initials Time	Checked By Initials Time	Checked By (If required) Initials Time					
3/7	DN 8:30	DN 8:40	CF 5:03						
3/8	NA			RV 5:27					
3/11	DN 3:00	DN 4:30							

After end-of-day check –

STORAGE CONTAINER CHECK SHEET									
From	Room No.	Building	Container No.	Certification					
	111A	3-100	123456	I certify, by my initials below, that I have opened, closed, or checked this storage container in accordance with pertinent agency regulations and operating instructions.					
Month/Year July 2013									
Date	Opened By Initials Time	Closed By Initials Time	Checked By Initials Time	Checked By (If required) Initials Time					
3/7	DN 8:30	DN 8:40	CF 5:03						
3/8	NA			RV 5:27					
3/11	DN 3:00	DN 4:30		TL 4:45					

2 Security Contact Numbers

NOTE: In the event of an imminent threat where someone needs help right away because of an injury or an immediate danger call 911.

2.1 Deployed Security Officer

Lori Koch
Email: tjkoch@lanl.gov
Office: 505-665-8801
Cell: 505-500-2859

2.2 Protective Force

2.2.1 *Central Alarm Station: 505-665-7708*

Shift Major: 505-665-1279
Security on Call Duty Officer (after hours/weekend reporting) Pager: 505-949-0156
Security Help Desk: 505-665-2002
Security Incident Team (SIT):
 Security Incidents: 505-665-3505
 Investigative Services: 505-665-6159

2.3 Personnel Security

Badge Office: 505-667-6901
Drug testing: 505-667-8378
LANL Emergency Operations Center: 505-667-2400
Los Alamos Police Department: 505-662-8222

2.4 Incident Reporting and Notifications web page

<https://int.lanl.gov/incident-reporting>

U.S. Department of Energy

Washington, D.C.

September 23, 2014

CLASSIFICATION BULLETIN

GEN-16 Revision 2: "NO COMMENT" POLICY ON CLASSIFIED INFORMATION IN THE OPEN LITERATURE

- I. PURPOSE. To provide guidance to DOE Federal and contractor employees authorized access to classified information (e.g., authorized person) on appropriate actions when unmarked documents, publications, or verbal comments containing classified information (i.e., Restricted Data (RD), Formerly Restricted Data (FRD), Transclassified Foreign Nuclear Information (IFNI), National Security Information (NSI)) or documents that are marked as containing classified information appear in the open literature and to clarify the circumstances that constitute comment.
- II. CANCELLATION. This bulletin supersedes GEN-16, Rev "'NO COMMENT' POLICY ON CLASSIFIED INFORMATION IN THE PUBLIC DOMAIN," dated August 31, 2011.
- III. RATIONALE. In today's information environment, it is likely that persons who are authorized access to classified information will encounter such information especially online in the open literature. DOE's goal is to avoid comment in order to minimize the damage to national security. Commenting on classified information in the open literature can cause risk of greater damage to the national security by confirming its location, classified nature, or technical accuracy. This bulletin establishes DOE standards for what constitutes a comment in regard to classified information.

Classified information can appear in the open literature in documents marked as classified that are generated by the Government. Classified information can also appear in the open literature in documents that are not generated by the Government and do not have any indication of the classification status of the information. Classification markings or the lack of classification markings do not always accurately reflect the classification status of information in the document. In order to maintain effective policies in an increasingly challenging information technology environment and for consistency with cybersecurity practice, this bulletin addresses classified information in the open literature contained in unmarked documents, as well as documents with classification markings.

IV. NATIONAL POLICY.

a. "No Comment" Policy. 10 CFR § 1045.22

- (1) Authorized holders of RD and FRD shall not confirm or expand upon the classification status or technical accuracy of classified information in the public domain.
- (2) Unauthorized disclosure of classified information does not automatically result in the declassification of that information.
- (3) If the disclosure of classified information is sufficiently authoritative or credible, the DOE Associate Under Secretary for Environment, Health, Safety and Security shall examine the possibility of declassification.

b. Executive Order 13526, Classified National Security Information, Part I, Section 1.1(c). "Classified information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information."

V. PRINCIPLES.

- ##### a. Comment. A comment is any activity that would allow a person who is not authorized access to classified information to locate the information or confirm the classified nature or technical accuracy of the information.

- b. Classification Status. An authorized person must not comment, either verbally or in writing, to a person who is not authorized access to classified information on the classification status of any classified information in the open literature (including the fact that a document is being reviewed for classification or the results of such a review, which may be disclosed only to the person who submitted the document for review).
- c. Technical Accuracy. An authorized person must not comment, either verbally or in writing, to a person who is not authorized access to classified information about the technical accuracy of classified information in the open literature.

VI. GUIDANCE.

- a. Guidance for Documents in the Open Literature that are Marked as Classified. Marked documents may appear in the open literature for several reasons. For example, they may have been leaked or they may have been appropriately declassified and released. In many cases, classification markings do not accurately convey the classification status of the document.

The markings may not be current and, unless the document is marked to indicate the document has been declassified, only an appropriate authority from the originating agency may determine the current classification status of the document. In cases where the classification status of marked documents in the open literature is ambiguous or unknown (e.g., declassification markings are not evident), the source must be treated as classified and the following guidance must be adhered to:

- (1) Viewing. Inadvertent viewing of such documents is not a comment unless instructions to the contrary are issued by the U.S. Government regarding a specific compromise.
- (2) Links. Links to such documents must not be forwarded via e-mail to any other person.
- (3) Printing. Such documents may only be printed on a printer that has volatile memory. When printed, the documents must be protected, as required.
- (4) Saving or Sending. The source itself must not be saved on an unclassified system or sent via e-mail to another person.

- b. Guidance for Documents Containing Classified Information in the Open Literature that are Not Marked. The following guidance provides clarification as to the activities that are or are not considered comment:
- (1) Viewing. Merely reading unmarked and unannotated documents or publications available in the open literature that contain classified information is not a comment unless instructions to the contrary are issued by the U.S. Government regarding a specific compromise.
 - (2) Collecting Publications or Internet Web Pages in a General Subject Area of Interest. Collecting unmarked and unannotated open literature publications or web pages in a given subject area or lists of open literature publications, assuming the title of that publication is not classified, is not a comment. Collections of topical news stories, favorite or bookmarked web sites, or listing of references do not by themselves constitute a comment. Basic summaries of collections of news articles may or may not constitute a comment depending on the content of the summary. Authorized persons must ensure that DOE classified information is not included within any summary of an open literature document. Authorized persons may collect open literature documents on such subjects as nuclear weapons, uranium centrifuges, etc., given that a variety of sources are widely available to the general public or to any informed researcher not authorized access to classified information, but they must not limit such collections only to open literature publications that contain classified information.
 - (3) Possessing, Printing, Saving, or Sending. The mere possession, printing, storage, or distribution of material from the open literature (e.g., books, news articles, links to Internet sites) that may contain classified information and are not marked as classified does not by itself add credibility to such material or constitute comment.
 - (4) Citing. Authorized persons may cite (e.g., in footnotes and bibliographies) well-known, unmarked open literature sources that contain classified information if the vast majority of the open literature document or publication does not contain classified information and the specific reference does not point to the classified information in the document. Authors must consult with their local Classification Officer for guidance on acceptable citations.

- (5) Annotating. Authorized persons must not annotate unmarked open literature material (including email containing such material or links to such material) to indicate in any way that the source contains classified information or that the section containing classified information is technically accurate. If authorized persons annotate an open literature source in a manner that does so, the annotated document must be reviewed by a Derivative Classifier and marked and protected at the level and category of the information as indicated in classification guidance.


- c. Unclassified Presentations and Discussions of a Classified Subject Area. When an authorized person is required as part of his or her official capacity to give presentations or hold discussions (e.g., press conference, town hall meeting, unclassified presentation, dialog with a technical expert who is not authorized access to classified information, etc.) in a classified subject area, the employee may comment if the employee knows that the specific information is unclassified.

WARNING: Selective use of "No Comment" may result in confirming classified information. Therefore, an authorized person should avoid commenting in such a manner that the use of "No Comment" would implicitly reveal that the information is classified. Employees should consider responding with a statement similar to "We do not comment on this type of information." for any questions concerning classified subject areas (e.g., yields, stockpile locations, etc.).

- d. Reporting. An employee encountering DOE classified information in the open literature must report the information following DOE policies and local instructions.
- e. Review of Documents that Potentially Contain Classified Information. Per DOE Order 475.2A, Identifying Classified Information, Attachment 4, I(a)(1), "Newly generated documents or material in a classified subject area that potentially contain classified information must receive a classification review by a Derivative Classifier." This requirement applies even if information contained in the document is taken from the Internet or another open literature source.

- VII. ADVISORIES. Advisories may be issued when an incident is particularly noteworthy or significant concerns regarding release of the classified information arise. It is not possible or advisable to distribute an advisory in all instances when classified information appears in the open literature. Whether or not an advisory is released, the "No Comment" policy should be followed whenever classified information appears in the open literature.

- VIII. EXCEPTIONS. Due to safety, environmental, public health, or other concerns, it may be necessary for the DOE to discuss documents in the open literature that contain classified information. Any official confirmation on the classification status or technical accuracy of information in the open literature is handled in accordance with DOE Order 471.6, Admin Chg. 1, *Information Security*, DOE Order 470.4B, Admin Chg. 1, *Safeguards and Security Program*, and any other applicable law, regulation, or policy.
- IX. VIOLATIONS. Any authorized person who intentionally verifies the classification status of any information or the technical accuracy of classified information in the open literature to a person not authorized access to classified information is subject to appropriate sanctions. Sanctions may range from administrative, civil, or criminal penalties, depending on the nature and severity of the action as determined by appropriate authority in accordance with applicable laws.
- X. CONTACT. Contact the Director, Office of Classification, (301) 903-3526, with any questions or comments concerning this bulletin.



Andrew P. Weston-Dawkes
Director
Office of Classification
Office of Environment, Health,
Safety and Security